

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----X
:
UNITED STATES OF AMERICA, :
:
:
- against - :
:
:
MICHAEL MENDLOWITZ, :
a/k/a "Moshe Mendlowitz," :
RICHARD D. HART, :
a/k/a "Rick Hart," :
:
Defendants. :
:
-----X

USDC SDNY
DOCUMENT
ELECTRONICALLY FILED
DOC #: _____
DATE FILED: 3/2/2019

17 Cr. 248 (VSB)

OPINION & ORDER

VERNON S. BRODERICK, United States District Judge:

The Indictment in this case charges Defendants Michael Mendlowitz and Richard Hart with three counts, including conspiracy to commit mail and wire fraud, mail fraud, and wire fraud, in violation of 18 U.S.C. §§ 1341 and 1343. Before me is (a) the motion submitted by Defendant Mendlowitz: (1) to suppress evidence obtained pursuant to a search warrant executed at Commerce Payment Group LLC; (2) for identification of *Brady* material; (3) for a bill of particulars; (4) for further identification of discovery to provide notice; and (5) for the production of lists of trial witnesses, trial exhibits, and co-conspirators at least 60 days prior to trial, and (b) Defendant Hart's motion for: (1) identification of *Brady* material; (2) a bill of particulars; (3) early disclosure of a witness list, material pursuant to 18 U.S.C. § 3500, and witness impeachment material; (4) disclosure of statements made by Defendant Mendlowitz; and (5) the disclosure of evidence pursuant to Federal Rule of Evidence 404(b). On January 10, 2019, Defendant Hart pled guilty thereby mooting—to the extent there might be any remaining issues after the May 16, 2018 conference during which I heard oral argument and issued an oral

decision (the “May 16 Conference”—further consideration of his motion. For the reasons outlined below, and explained on the record during the May 16, 2018 conference, Defendant Mendlowitz’s motion is GRANTED IN PART AND DENIED IN PART.

I. Background

A. *The Alleged Scheme*¹

From 2009 to July 2015, Defendants, as executives of Commerce Payment Group LLC (“CPS”—a credit card processing company—defrauded CPS customers, including small merchants who accepted credit cards and debit cards at their businesses. (Indictment ¶ 2.) Mendlowitz was the president and chief executive officer (“CEO”) of CPS, and a minority owner of a twenty percent share of the company. (*Id.* ¶ 12.) Hart held various executive titles at the company until the termination of his employment in February 2015. (*Id.* ¶ 13.)

More specifically, the Indictment alleges that Defendants used CPS’s marketing and sales staff to falsely represent to prospective customers that they could obtain bankcard-processing services at rates below those of CPS’s competitors, with no hidden fees or extra charges, and with guarantees that the rates would never change. These false rates and other misrepresented rates were then partially reflected in written agreements with customers, often with large discrepancies between the fees represented orally, those represented in written agreements, and those that CPS actually charged. Defendants purportedly caused CPS to use deceitful accounting tricks to bill customers above the rates represented and agreed upon, to impose extra fees, and to engage in multiple billing. For example, some “transaction fees” were charged multiple times on a single transaction while other fees were charged at ten times the contract rate—e.g., an

¹ The facts contained in this section are taken from the allegations in the Indictment filed in this case on April 24, 2017. (Doc. 2.)

assessment quoted at .095% might be billed at 0.95%. By using these tactics and others, Defendants allegedly collected \$30 million over the course of two and a half years. (*Id.* ¶¶ 16–27.)

B. *The Search Warrant*

On July 23, 2015, Magistrate Judge Steven Gold of the U.S. District Court for the Eastern District of New York issued a search warrant (the “Search Warrant” or “Warrant”) authorizing a search of CPS at its offices located in an office building at 1465 Broadway, Hewlett, New York (the “CPS Premises” or as defined in the Warrant “Subject Premises”). (SW 1.)² The Search Warrant contains a description of the premises to be searched, along with a map and photographs of the building’s exterior. (*See generally id.*) It authorized agents to search the CPS Premises and to seize “evidence, fruits, and instrumentalities of the operation of a fraudulent credit-card and debit-card processing scheme, in violation of Title 18, United States Code, Sections 1343 and 1349.” (*See id.*, Attach. B.) More specifically, the warrant authorized agents to seize twelve specified categories of evidence and instrumentalities of the alleged bankcard-processing scheme, including:

1. Business and financial reports and records, bank and credit card records, customer contracts and applications, customer bills, customer billing profiles, sales and debt-collection records, employee records and files, call logs, call lists, service and other contracts, recorded telephone calls, creditor and debtor records, internal and external correspondence and communications, mail, and payment records, among other documents, stored media and records;
2. Checks (personal and certified), customer contracts and agreements, customer bills, copies of canceled checks, cash, money orders, records of credit card payments, mail, mail envelopes, correspondences, communications, faxes, emails, phone records (including digital and/or VOIP records), receipts, invoices, general journals, ledgers, financial reports, spreadsheets, memoranda,

² “SW” refers to the July 23, 2015 Search and Seizure Warrant, 15M0688, attached as Exhibit 3 to the Declaration of Patrick J. Smith in support of the Memorandum of Law in Support of Defendant Michael Mendlowitz’s Motion to Suppress. (Doc. 54-4.)

and notes;

3. Bank account and transaction documents, including account opening documents, ATM and/or debit cards, bank statements, and bank deposit and withdrawal slips;
4. Customer and/or debtor lists, customer and/or debtor files, lists of names, addresses, social security numbers, contact information, bank account numbers, credit card numbers and other personal identifying information, records of communications with customers and/or debtors;
5. Company policies, manuals, instructions, and/or scripts;
6. Any documents mentioning arrests and/or warrants;
7. Licenses and/or registrations;
8. Documents, records and policies regarding employee compensation, such as bonuses and/or commissions;
9. Payroll records, employee names, personnel files;
10. Documents or records bearing the names “Commerce Payment Systems,” “Commerce Payment Group,” “Merchant Commerce,” “Empire Payments,” “Evolution Bankcard,” “Optimal Bankcard,” “EVO Merchant Services,” “EVO Payments International,” “Michael Mendlowitz,” or similar names;
11. Records relating to and communications regarding lenders, creditors and/or other sources of information regarding debtors or debts to be collected; and
12. Computer(s), computer hardware, software, related documentation, and passwords.

(*Id.*)

The Search Warrant also provided that the “items to be seized from the Subject Premises also include any computer devices and storage media that may contain any electronically stored information” (“ESI”) falling within the twelve enumerated categories of evidence. (*See id.*, Attach. C.) The Search Warrant described the different techniques that authorities could use to conduct a review of seized ESI, including “performing key word searches,” and provided that “law enforcement personnel are authorized to conduct a complete review of all the ESI . . . if

necessary to evaluate its contents and to locate all data responsive to the warrant.” (*See id.*, Attach. B.)

The Search Warrant was supported by a 46-page affidavit of United States Secret Service Agent Brandon McCaw (the “Search Warrant Affidavit”). The information contained in the Search Warrant Affidavit came from various individuals and documents, including: (1) a confidential witness (“CW-1”) and a confidential source (“CS-1”)³, both of whom had admitted to participating in the fraudulent scheme; (2) complaints filed by CPS merchant-customers with government agencies and consumer complaint organizations; (3) public records; (3) bank records; (4) fraudulent CPS customer bills; and (5) customer agreements. (SW Aff. ¶ 5.)⁴ The Search Warrant Affidavit detailed the use by Defendants and their co-conspirators of internet websites, in-house computer systems, emails, recorded telephone calls, sales scripts, and uniform and agreed upon false statements to prospective customers, and described an array of fraudulent practices employed by Defendants and their co-conspirators, including overbilling commission fees, improperly charging fees multiple times, charging fees that customers were told they would not be charged, charging inapplicable and large surcharges, and defrauding customers even after they sought refunds or cancellations. (*Id.* ¶¶ 6–8, 18–22.) Furthermore, the Search Warrant Affidavit described the ESI that Special Agent McCaw anticipated would be found at the CPS offices, detailing the ways in which employees at CPS along with its parent company and others used its computer systems, servers, electronic media, emails and attachments, web-based

³ Prior to the preparation of the Search Warrant Affidavit, CW-1 had pled guilty to participating in the fraud scheme, while CS-1 had been arrested and was cooperating with the Government but had not yet pled guilty. CS-1 subsequently pled guilty to participating in the scheme. (Gov. Mem. 7.) “Gov. Mem.” refers to the Government’s Memorandum of Law in Opposition to Defendants’ Pretrial Motions, filed on March 8, 2018. (Doc. 61.)

⁴ “SW Aff.” refers to the affidavit of U.S. Secret Service Special Agent Brandon McCaw submitted in support of the application for Search and Seizure Warrant 15M0688, attached as Exhibit 4 to the Declaration of Patrick J. Smith in support of the Memorandum of Law in Support of Defendant Michael Mendlowitz’s Motion to Suppress. (Doc. 54-5.)

software and links, electronically recorded telephone conversations, and electronic communications. (*Id.* ¶¶ 32–38.)

C. *The Search of the CPS Premises*

Agents executed the Search Warrant on July 28, 2015 and seized approximately 2,700 pages of paper files, including contracts, correspondence, banking records, sales scripts, and other perceived evidence of the fraud. (Gov. Mem. 9.) With regard to ESI, agents found both a server room containing CPS’s computer servers, as well as dozens of individual employee offices and workstations containing personal desktop computers, laptop computers, and other data storage devices. (*Id.* at 9–10.) Among the dozens of CPS employee workstations encountered, agents seized devices belonging to five employees, as well as two electronic devices from Mendlowitz’s desk. (*Id.* at 10.)

D. *Review of the Seized Material*

Following the execution of the Search Warrant, the Government undertook a review of the seized ESI, focusing primarily on three CPS servers and three CPS desktop computers, including the two computers taken from Mendlowitz’s workspace. (*Id.* at 33–34.) Prior to reviewing the ESI, the Government copied the files onto several different text-searchable platforms. (*Id.* at 34.) In undertaking its review, the Government used two separate techniques, yielding two different groups of documents identified as potentially responsive to the Warrant. The first technique involved individuals reviewing the seized material identifying specific individuals’ emails and documents, all of which were identified as potentially responsive. (See Lewis Aff. Ex. C (Government’s March 6, 2018 discovery letter); Smith Dec. Ex. 12 (Government’s November 30, 2017 discovery letter).)⁵ With regard to the second technique,

⁵ “Lewis Aff.” refers to the Mach 8, 2018 Affirmation of David Raymond Lewis, filed in support of the Government’s Memorandum of Law in Opposition to Defendants’ Pretrial Motions. (Doc. 62.) “Smith Dec.” refers

reviewing personnel used key-word computerized searches to identify and compile collections of emails containing certain search terms. (Gov. Mem. 35.) The Government then subjected the collections gathered using the two techniques to individualized review, identifying individual emails and documents that were then identified and marked as responsive. (*Id.*) By the conclusion of the review process, and prior to the return of the Indictment in April 2017, the Government identified roughly 1,830 responsive documents. (*See* Lewis Aff. Ex. C; Smith Dec. Ex. 12.) On November 30, 2017, the Government produced both the collections of documents that had been identified as potentially responsive, and the 1,830 individually identified emails and other documents identified as responsive.

With regard to the timing of the review process, the Government began its review in approximately October 2015, two months after the execution of the Search Warrant and after the relevant portions of the hard drives had been copied onto text-searchable software platforms, and completed the review before the return of the Indictment in April 2017. (*See* Smith Dec. Ex. 9.) The Government represents that it has not engaged in any review of the non-responsive ESI since the date of the Indictment, and has informed defense counsel that it is prepared to stipulate that the only responsive documents—assuming no additional search warrant is obtained—are those 1,830 files that have been individually identified. (*See* Lewis Aff. Ex. C.)

Following the search, the Government was contacted by CPS attorneys regarding the return of certain ESI and hardware.⁶ (Gov. Mem. 37–38.) On October 13, 2015, counsel for CPS provided the Government with a formal request for the return of mirror images of three CPS

to the January 22, 2018 Declaration of Patrick J. Smith, filed in support of the Memorandum of Law in Support of Defendant Michael Mendlowitz's Motion to Suppress, for Return of Property, for Identification of Brady Material and for a Bill of Particulars. (Doc. 54.)

⁶ CPS was represented by Ropes & Gray LLP, not counsel for Mendlowitz or Hart. (Lewis Aff. Ex. L.)

servers, as well as the original servers (minus their hard drives), and on or about October 14, 2015, the Government complied with that request. (Lewis Aff. ¶ 13, Ex. M.)

II. Procedural History

The Indictment was returned on April 24, 2017. (Doc 2.) On January 18, 2018, Defendant Hart filed his motion, along with a memorandum and declaration of Eric Sears in support. (Docs. 46–48.) On January 22, 2018, Defendant Mendlowitz filed his motion, along with a memorandum and the declaration of Patrick J. Smith in support with exhibits. (Docs. 52–54.) On March 8, 2018, the Government filed an opposition to Defendants' motions, along with the affirmation of David Lewis in support with exhibits. (Docs. 61–62.) On March 29, 2018, Mendlowitz filed a reply in support of his motion, along with the declaration of Rodney Villazor in support with exhibits. (Docs. 66, 69.)

On May 16, 2018, I held a status conference in this matter. During the conference I made the following rulings on Defendants' motions: I denied Defendants' motions for a bill of particulars and for identification of *Brady* material, and denied Defendant Hart's motion for early disclosure of 18 U.S.C. § 3500 material and witness impeachment material; I granted in part and denied in part Defendants' motions for the early production of lists of trial witness and trial exhibits; and I granted Defendant Hart's motion for the early disclosure of evidence pursuant to Federal Rule of Evidence 404(b) and Defendant Mendlowitz's motion for a list of co-conspirators. (Doc. 77; *see also* Doc. 76.) I also denied Defendant Mendlowitz's motion to suppress evidence obtained pursuant to the Search Warrant and, with respect to that ruling, indicated that I would follow my decision on the record with a written opinion. (Doc. 77.)

III. Discussion

I now address in further detail my denial of Mendlowitz’s motion to suppress the Search Warrant on the basis that his Fourth Amendment rights were violated. Mendlowitz insists that the Warrant suffers from two fatal flaws that transformed it into a general warrant and provide grounds for suppression. First, he claims that the Warrant lacks particularity and that it neither adequately describes the subject offenses nor gives unambiguous guidance as to what evidence could be seized. Second, he argues that the continued retention and untimely searches of ESI exceed the limits of Fourth Amendment reasonableness. As a threshold matter, the Government contends that Mendlowitz has not established that his own Fourth Amendment rights were violated by the challenged search and seizure. I address these arguments in turn below.

A. *Reasonable Expectation of Privacy*

The Government contends that Mendlowitz’s motion fails because he cannot demonstrate a reasonable expectation of privacy in the CPS computer servers and desktop computers located at the workstations of various CPS employees, and the desktop computers that were located in his own office. (Gov. Mem. 10–11.) In response, Mendlowitz argues that “as a co-owner, president and CEO who was actively involved in the day-to-day operations at the CPS Premises, and who had possession of the CPS Premises as a matter of both legal right and practical access, [he] had a reasonable expectation of privacy within the entire CPS Premises and the ESI located on CPS computers.” (Mendlowitz Reply 2.)⁷ For the reasons stated on the record during the May 16, 2018 status conference and outlined below, I find that Mendlowitz has demonstrated a reasonable expectation of privacy sufficient to challenge the search of his own office, including

⁷ “Mendlowitz Reply” refers to the Reply Memorandum of Law in Further Support of Defendant Michael Mendlowitz’s Motion to Suppress, for Return of Property, for Identification of Brady Material, and for a Bill of Particulars, dated March 29, 2018. (Doc. 66.)

items that may have been saved on the hard drive of his desktop computers, but not of the materials saved on CPS's computer servers or the computers of other CPS employees.

1. Applicable Law

According to the Fourth Amendment, “no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. “A defendant seeking to suppress the fruits of a search by reason of a violation of the Fourth Amendment must show that he had a ‘legitimate expectation of privacy’ in the place searched.” *United States v. Hamilton*, 538 F.3d 162, 167 (2d Cir. 2008) (quoting *Rakas v. Illinois*, 439 U.S. 128, 143 (1978)); *see also United States v. Villegas*, 899 F.2d 1324, 1333 (2d Cir. 1990) (“A defendant has no right to have evidence suppressed on Fourth Amendment grounds unless the breached privacy expectation was his own rather than that of a third party.”). “This inquiry involves two distinct questions: first, whether the individual had a subjective expectation of privacy; and second, whether that expectation of privacy is one that society accepts as reasonable.” *Hamilton*, 538 F.3d at 167 (citing *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

It is axiomatic that “the proponent of a motion to suppress has the burden of establishing that his own Fourth Amendment rights were violated by the challenged search or seizure.” *Rakas*, 439 U.S. at 130 n.1. Accordingly, a defendant asking a court to suppress evidence must demonstrate a legitimate expectation of privacy in the area that was searched. *See, e.g., id.*; *Rawlings v. Kentucky*, 448 U.S. 98, 104 (1980). “Where the premises searched is a business, defendants seeking suppression must establish both that they are associated with the business and that they have a legitimate expectation of privacy in the part of the business that was searched.” *United States v. Kazarian*, No. 10 Cr. 895(PGG), 2012 WL 1810214, at *18 (S.D.N.Y. May 18,

2012) (citing *O'Connor v. Ortega*, 480 U.S. 709, 718 (1987)). Unlike the nearly absolute protection of a residence, the “great variety of work environments” requires analysis of reasonable expectations “on a case-by-case basis.” *O'Connor*, 480 U.S. at 718.

2. Application

Mendlowitz points to no facts sufficient to support his assertion that he had a reasonable expectation of privacy in the corporate servers or the CPS desktop computers seized from locations other than his own office. Mendlowitz merely asserts that he maintained a reasonable expectation of privacy with regard to the entirety of the CPS facility due to his role as the co-owner, president, and CEO of the company. However, courts routinely find that owners and executives of companies do not have reasonable expectations of privacy in general business records when they fail to demonstrate a subjective expectation of privacy in those records.

In *United States v. Chuang*, the defendant served as the chairman, president, and CEO of Golden Pacific National Bank, and owned with his family nearly half of the shares of the bank and “exercised significant operational control over the bank and all of its premises.” 897 F.2d 646, 650 (2d Cir. 1990). Chuang, in challenging the pretrial denial of his suppression motion of the search of the bank and the resulting seizure of electronic materials before the Second Circuit, argued that as a corporate officer he had established a sufficient expectation of privacy in the bank premises to challenge the legality of the search. *Id.* The Second Circuit disagreed, denying Chuang’s attempt to suppress the evidence, noting that “the bulk of the bank documents” were seized from the office of another officer of the bank, and finding that Chuang “failed to demonstrate a sufficient nexus between the areas from which the documents were obtained and his own office.” *Id.*⁸ In other words, Chuang failed to establish a sufficient showing of a

⁸ The court also found, as an additional reason to deny suppression, that Chuang failed to demonstrate an expectation of privacy that society considers reasonable because he worked in a “closely regulated industr[y]” and

possessory or proprietary interest in the area where the documents were found. Other courts have reached similar conclusions. *See, e.g., United States v. Nagle*, 803 F.3d 167, 178–79 (3d Cir. 2015) (finding that majority owner of company who sought suppression of evidence seized by search warrant from corporate servers and offices of other employees had no expectation of privacy in the offices of others and that, even as to his own emails on the corporate servers, had failed to show a subjective expectation of privacy); *United States v. SDI Future Health, Inc.*, 568 F.3d 684, 694, 698 (9th Cir. 2009) (denying challenge of business owners to search of corporation’s premises because mere ownership and management is insufficient to challenge search, but finding that defendants could show a legitimate expectation of privacy in corporation’s property if they “show[ed] some personal connection to the places searched and the materials seized” and “took precautions on [their] own behalf to secure the place searched or things seized from any interference without [their] authorization”); *Williams v. Kunze*, 806 F.2d 594, 594, 599–604 (5th Cir. 1986) (concluding that sole shareholder of corporation lacked standing where “the vast majority of documents seized . . . were corporate records” rather than personal files and defendant “had no reasonable expectation of privacy in corporate records maintained in a common file room”); *United States v. Britt*, 508 F.2d 1052, 1055–56 (5th Cir. 1975) (finding lack of standing where shareholder and president of corporation did not personally use the space searched and materials seized were “normal corporate records”).⁹

that, as a result, Chuang “knew that bank documents, whether kept in his office or another office, were subject to periodic examination.” *Chuang*, 897 F.2d at 650.

⁹ I note also that a defendant seeking to challenge a search of corporate offices usually must submit an affidavit showing that he had a reasonable expectation of privacy in the area searched or items seized. *See United States v. Tranquillo*, 606 F. Supp. 2d 370, 378 (S.D.N.Y. 2009) (“As a preliminary matter, [defendant] has not put forth the foregoing facts—or, indeed, *any* facts relevant and probative of his privacy interest in the [seized computers]—in a sworn affidavit.”); *United States v. Sorcher*, No. 05 CR 0799 NG RLM, 2007 WL 1160099, at *8 (S.D.N.Y. Apr. 18, 2007) (“Indeed, the record contains no affidavits from defendants asserting their possessory or proprietary interest in the documents.”). No affidavit has been submitted in this case. Instead, Mendlowitz offers only unsworn statements of counsel. This failure alone is sufficient to deny Mendlowitz’s motion to suppress. However, I will assume Mendlowitz has adequately alleged standing and address the substance of Mendlowitz’s suppression motion.

The cases cited by Mendlowitz are not to the contrary and do not support a different conclusion. (See Mendlowitz Mem. 26.)¹⁰ In *United States v. Schwimmer*, 692 F. Supp. 119 (E.D.N.Y. 1988), where the defendant was the sole shareholder of the company searched, the court declined to reach the issue of standing, finding that “[i]n order to dispose of this motion without an evidentiary hearing, I will assume that [the defendant] has shown a privacy interest in the searched premises and seized property, and will move on to the issue of probable cause.” *Id.* at 125. Moreover, *United States v. Zemlyansky*, 945 F. Supp. 2d 438 (S.D.N.Y. 2013), does not provide any support since although the court found the corporate officer defendants had standing it provided no explanation of its analysis and cited no case law in support of its conclusion. *See id.* at 452.

With regard to the search and seizure of the computers from Mendlowitz’s own workspace, I find that Mendlowitz has established a sufficient privacy interest to maintain a challenge to the search. While the extent to which an employee may challenge a search of business premises generally is nuanced, courts agree that an employee may contest the search of his private office. *See, e.g., Mancusi v. DeForte*, 392 U.S. 364, 369 (1968) (“It has long been settled that one has standing to object to a search of his office.”); *Chuang*, 897 F.2d at 649 (“It is well-settled that a corporate officer or employee in certain circumstances may assert a reasonable expectation of privacy in his corporate office.”); *Kazarian*, 2012 WL 1810214, at *18 (“There is no dispute here that [defendant] has standing to challenge the search of his residence and office.”).

I also note that the Government does not challenge the location of Mendlowitz’s workspace and the fact that two computers were found in that space. (Gov. Mem. 10.)

¹⁰ “Mendlowitz Mem.” refers to the Memorandum of Law in Support of Defendant Michael Mendlowitz’s Motion to Suppress, for Return of Property, for Identification of Brady Material and for a Bill of Particulars, filed on January 22, 2018. (Doc. 53.)

Although the Government contends that Mendlowitz has no legitimate expectation of privacy in the contents of the computers from his desk because CPS had a policy notifying employees that such contents and communications are not private, (Gov. Mem. 16), I find the cases cited by the government in support of that position are (1) not binding on me, (2) distinguishable, and/or (3) inapposite under the circumstances presented in this case. *See United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000) (pertaining to warrantless search conducted by employer); *United States v. Nordlicht*, No. 16-cr-00640 (BMC), 2018 WL 705548, at *4 (E.D.N.Y. Feb. 2, 2018) (finding lack of expectation of privacy based on communication policy in employee handbook in case brought by employees as opposed to co-owner, president, or CEO); *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548, 560–61 (S.D.N.Y. 2008) (ruling in a civil trademark infringement case that employer’s access of employee’s personal e-mails was unauthorized); *Williams v. Rosenblatt Sec. Inc.*, 136 F. Supp. 3d 593, 607 (S.D.N.Y. 2015) (concluding in a civil whistleblower matter that employer’s access of terminated employee’s emails was not statutorily improper); *cf. Leventhal v. Knapek*, 266 F.3d 64, 74–75 (2d Cir. 2001) (holding that employee had reasonable expectation of privacy in the contents of his own office computer where there was no clear policy regarding regular monitoring of work computers but employer conducted periodic searches).¹¹

Accordingly, I find that Mendlowitz has demonstrated a sufficient privacy interest with regard to the materials seized from his office and computers but not with regard to the computers

¹¹ Mendlowitz argues that the Government improperly used the grand jury to obtain a copy of the CPS employee handbook as a means to gather evidence in opposition to Mendlowitz’s motion. (Mendlowitz Reply 3 n.2.) Because I find that Mendlowitz has standing to assert a Fourth Amendment claim over the materials seized from his office, and do not rely on the employee handbook to find otherwise, I do not address this argument. Furthermore, I note that arguments raised in footnotes need not be addressed. *See, e.g., Diesel v. Town of Lewisboro*, 232 F.3d 92, 110 (2d Cir. 2000) (“We do not consider an argument mentioned only in a footnote to be adequately raised” (internal quotation marks omitted)); *Levy v. Young Adult Institute*, 103 F. Supp. 3d 426, 441 (S.D.N.Y. 2015) (denying consideration of argument raised in footnote in reply brief).

and materials seized from the offices of other employees or the CPS servers generally.

B. *Particularity of the Search Warrant*

Mendlowitz maintains that the Search Warrant lacked particularity because it failed to provide sufficient guidance as to the fraud allegedly perpetrated and the evidence to be seized, and that the fruits of the Search Warrant should be suppressed as a result. In response, the Government argues that the Search Warrant was fully compliant with the Fourth Amendment and, even if it was not, the good faith doctrine would preclude suppression.

1. Applicable Law

a. Fourth Amendment Particularity

As previously discussed, the Fourth Amendment requires, among other things, that search warrant affidavits “particularly describe[e] the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV; *see also United States v. Hernandez*, No. 09 CR 625(HB), 2010 WL 26544, at *7 (S.D.N.Y. Jan. 6, 2010) (“A warrant . . . can be unconstitutionally infirm in two conceptually distinct but related ways: either by seeking specific material as to which no probable cause exists, or by giving so vague a description of the material sought as to impose no meaningful boundaries.” (internal quotation marks omitted)). The particularity requirement “guards against general searches that leave to the unguided discretion of the officers executing the warrant the decision as to what items may be seized.” *United States v. Riley*, 906 F.2d 841, 844 (2d Cir. 1990); *see also United States v. Clark*, 638 F.3d 89, 94 (2d Cir. 2011) (“Particularity concerns frequently arise in circumstances where the description in the warrant of the place to be searched is so vague that it fails reasonably to alert executing officers to the limits of their search authority[.]”). In other words, “[p]articularity is the requirement that the warrant must clearly state what is sought.” *United States v. Jacobson*, 4 F. Supp. 3d 515, 521 (E.D.N.Y. 2014). “To

be sufficiently particular under the Fourth Amendment, a warrant must satisfy three requirements.” *United States v. Ulbricht*, 858 F.3d 71, 99 (2d Cir. 2017). The warrant must: (1) “identify the specific offense for which the police have established probable cause”; (2) “describe the place to be searched”; and (3) “specify the items to be seized by their relation to designated crimes”. *Id.* (internal quotation marks omitted).

The level of specificity required by the Fourth Amendment depends on many factors, *Jacobson*, 4 F. Supp. 3d at 522, and “does not require a perfect description of the data to be searched and seized,” *Ulbricht*, 858 F.3d at 100. Indeed, “[s]earch warrants covering digital data may contain some ambiguity.” *Id.* (internal quotation marks omitted). In instances in which complex crimes are alleged, “it may be appropriate to use more generic terms to describe what is to be seized.” *United States v. Gotti*, 42 F. Supp. 2d 252, 274 (S.D.N.Y. 1999); *see also Jacobson*, 4 F. Supp. 3d at 522 (concluding that broad warrant was justified because “the crimes under investigation were complex and concerned a long period of time, not simply one or two dates of criminal activity”); *United States v. Levy*, No. S5 11 Cr. 62(PAC), 2013 WL 664712, at *9 (S.D.N.Y. Feb. 25, 2013) (noting that “[w]hile some of the categories are somewhat vague, given the complexity of the alleged scheme and the numerous documents involved, the lists of items are described with as much particularity as circumstances reasonably allowed” (internal quotation marks omitted)), *aff’d*, 803 F.3d 120 (2d Cir. 2015). In other words, “a search warrant does not necessarily lack particularity simply because it is broad.” *Ulbricht*, 858 F.3d at 100.

Furthermore, when a search warrant limits the scope of the search to evidence of particular federal crimes, and gives an “illustrative list of seizable items,” courts typically find the search warrant to be sufficiently particular. *See Riley*, 906 F.2d at 844–45. Likewise, courts often find that a warrant authorizing the seizure of “all evidence” of a given crime is sufficiently

particular if it includes a list of illustrative items. *See, e.g., id.* (finding that warrant containing list of illustrative items to seize was sufficiently particular notwithstanding provision allowing seizure of “other items that constitute evidence of the offenses”); *United States v. Young*, 745 F.2d 733, 759–60 (2d Cir. 1984) (concluding that warrant allowing seizure of listed items plus “other evidence” of the specified crimes was sufficiently particular).

In addition, a warrant may leave some matters to the discretion of the executing officer. “Once a category of seizable papers has been adequately described, with the description delineated in part by an illustrative list of seizable items, the Fourth Amendment is not violated because the officers executing the warrant must exercise some minimal judgment as to whether a particular document falls within the described category.” *Riley*, 906 F.2d at 845. In short, the particularity requirement is satisfied if the warrant enables the executing officer to ascertain and identify with reasonable certainty those items that the magistrate judge has authorized him or her to seize. *See Groh v. Ramirez*, 540 U.S. 551, 557–58 (2004).

b. Good Faith Exception

“The fact that a Fourth Amendment violation occurred . . . does not necessarily mean that the exclusionary rule applies.” *Herring v. United States*, 555 U.S. 135, 140 (2009). The Supreme Court has explained that application of the exclusionary rule has always been its “last resort,” not its “first impulse.” *Id.* “To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system.” *Id.* at 144.

Under the good faith exception, the exclusionary rule does not apply to “evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant.” *United States v. Leon*, 468 U.S. 897, 922 (1984). “The burden is on the government to

demonstrate the objective reasonableness of the officers' good faith reliance on an invalidated warrant." *United States v. Clark*, 638 F.3d 89, 100 (2d Cir. 2011) (internal quotation marks omitted). "In assessing whether it has carried that burden," courts must be "mindful that, in *Leon*, the Supreme Court strongly signaled that most searches conducted pursuant to a warrant would likely fall within its protection." *Id.*; *see also Leon*, 468 U.S. at 922 ("Searches pursuant to a warrant will rarely require any deep inquiry into reasonableness, for a warrant issued by a magistrate normally suffices to establish that a law enforcement officer has acted in good faith in conducting the search.") (internal quotation marks omitted)). Thus, "[m]ost searches will be upheld." *United States v. Rickard*, 534 F. App'x 35, 37 (2d Cir. 2013) (summary order). As the Second Circuit has explained:

It was against this presumption of reasonableness that the Supreme Court identified four circumstances where an exception to the exclusionary rule would not apply: (1) where the issuing magistrate has been knowingly misled; (2) where the issuing magistrate wholly abandoned his or her judicial role; (3) where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable; and (4) where the warrant is so facially deficient that reliance upon it is unreasonable.

Clark, 638 F.3d at 100 (internal quotation marks omitted).

2. Application

a. Particularity

Mendlowitz argues that the Warrant lacked particularity because it purportedly authorized a general search of the CPS Premises for evidence. Mendlowitz is wrong. The Search Warrant was sufficiently particularized as it identified the specific offense, the place to be searched, and the items to be seized. *See Ulbricht*, 858 F.3d at 101 (observing that "the warrant plainly satisfies the basic elements of the particularity requirement" because the warrant "lists the charged crimes, describes the place to be searched, and designates the information to be

seized in connection with the specified offenses”). Rather than authorizing the agents to seize “every scrap of paper and byte of data,” (Mendlowitz Mem. 13), the Warrant limited the scope of the materials to be seized to twelve categories of documentary evidence that constituted “evidence, fruits, and instrumentalities of the operation of a fraudulent credit-card and debit-card processing scheme in violation of Title 18, United States Code, Sections 1343 and 1349.” (SW Attach. B.) Unlike a search warrant that allows “general, exploratory rummaging,” *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971), or one that only contains “general boilerplate terms, without either explicit or implicit limitation on the scope of the search,” *United States v. Buck*, 813 F.2d 588, 591 (2d Cir. 1987), the Warrant directed and limited executing agents to seize specific categories of evidence of the particular bankcard-processing scheme at issue. Indeed, every sub-paragraph of the list of evidence to be seized is modified by introductory language limiting the search to evidence of the scheme and thus ensures that each category of evidence was expressly limited to the specified crimes at issue. *See Hernandez*, 2010 WL 26544, at *10 (“The search warrant . . . is sufficiently particularized in terms of the types of documents to be seized [because the] warrant itself indicates that only documents related to violations of various criminal fraud statutes related to identity, mail, and tax fraud [may be seized].”).

Moreover, warrants—like the Warrant here—authorizing the seizure of any and all evidence of specified crimes, “including but not limited to” illustrative categories of documents and records are often found to be proper. Courts routinely validate such warrants in the face of particularity challenges, reasoning that an illustrative list, coupled with a reference to the crimes for which evidence is sought, supplies sufficiently limiting guidance. *See, e.g., Riley*, 906 F.2d at 844–45; *Young*, 745 F.2d at 759–60; *United States v. Lustyik*, 57 F. Supp. 3d 213, 227–28 (S.D.N.Y. 2014) (opining that warrant permitting seizure of all “evidence, fruits, or

instrumentalities” of specified crimes was sufficiently particular because it contained “an illustrative list of items to be seized,” even though illustrative list was preceded by phrase “including but not limited to” (internal quotation marks omitted)); *Jacobson*, 4 F. Supp. 3d at 524–25 (upholding warrant for “[a]ny and all records, data and correspondence constituting evidence, fruits and instrumentalities of” specified crimes, “in any form wherever that they may be stored or found including, but not limited to” specified categories); *cf. Buck*, 813 F.2d at 591 (finding warrant permitting seizure of “any papers, things or property of any kind relating to” specified crime to be insufficiently particular because it was unaccompanied by an illustrative list). I find that there is no legal or factual basis to depart from the reasoning of this line of cases.

The Warrant in this case materially differs from those in the cases upon which Mendlowitz relies. In *United States v. Wey*, in finding that the warrant lacked sufficient particularity, the court expressly noted that the warrants there “fail[ed] to set forth the crimes under investigation” and failed to “cite criminal statutes.” 256 F. Supp. 3d 355, 384 (S.D.N.Y. 2017). Neither is true of the instant Search Warrant, which explicitly limited the search to evidence of a particular fraud scheme in violation of particular statutes. Likewise, in *Zemlyansky*, the court relied in part on the fact that the warrant failed to “inform[] the searching officer for which crimes the search [was] being undertaken The officers are thus directed to these categories without a single word of guidance regarding the type of criminal offense under investigation.” 945 F. Supp. 2d at 454; *see also United States v. Vilar*, No. S305CR621KMK, 2007 WL 1075041, at *22 (S.D.N.Y. Apr. 4, 2007) (“[W]arrants are generally found to be insufficiently particular where nothing on the face of the warrant tells the searching officers for what crime the search is being undertaken.” (internal quotation marks omitted)). Therefore, I find that these cases are not instructive under the circumstances of these case.

Based on the foregoing, I find that the documents specified in Attachment B as incorporated by the Search Warrant were sufficiently particular to allow government agents to perform a discrete search for relevant evidence of the specific fraudulent scheme.

b. Good Faith

Even if I were to determine that the Search Warrant was insufficiently particular, the good faith exception would preclude suppression. Pursuant to *Leon*, the exception protects from suppression a search and seizure made in good faith reliance by government agents based on a search warrant in all but four situations: “(1) where the issuing judge has been knowingly misled; (2) where the issuing judge wholly abandoned his or her judicial role; (3) where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable; and (4) where the warrant is so facially deficient . . . that reliance upon it is unreasonable.”

United States v. Falso, 544 F.3d 110, 125 (2d Cir. 2008) (internal quotation marks omitted).

None of these factors exists here.

Mendlowitz neither suggests, nor has any basis to suggest, that Magistrate Judge Gold abandoned his judicial role or was misled by the case agent. *See Clark*, 638 F.3d at 100. Nor can it be said that the Search Warrant Affidavit was so lacking in indicia of probable cause as to render reliance upon it unreasonable.¹² *See, e.g., United States v. Scully*, 108 F. Supp. 3d 59, 104 (E.D.N.Y. 2015) (finding that search warrants were supported by probable cause where “affidavits made allegations against [defendants] stating that they were potentially engaging in criminal conduct, including selling misbranded and unapproved drugs [and] related in detail the

¹² Although I was required to assess the facial validity of the Warrant independently of the unattached Search Warrant Affidavit, unincorporated affidavits are “still relevant to [a court’s] determination of whether the officers acted in good faith,” to the extent the officers searched for evidence based on the affidavit’s probable cause statement. *See United States v. Rosa*, 626 F.3d 56, 64 (2d Cir. 2010). Mendlowitz does not dispute this point. (See Mendlowitz Reply 11.)

underlying investigation; including the undercover calls; . . . the undercover purchases; [etc.]”).

Indeed, Mendlowitz does not challenge the Search Warrant on the basis that it lacked probable cause.

Finally, the instant Warrant cannot be described as so facially deficient that reliance upon it was unreasonable. Courts have “illustrate[d] that a warrant is facially defective when it omits or misstates information specifically required to be contained therein, i.e., the place to be searched, and the persons or things to be seized.” *Clark*, 638 F.3d at 102 (internal quotation marks omitted); *see also Hernandez*, 2010 WL 26544, at *12 (finding that search warrant was not so facially deficient as to render reliance unreasonable because “[g]iven the nature of a complex tax fraud case like this one, a government agent would likely expect to find fairly broad categories of tax-related documents to be seized”). This is not the case with the Warrant.

Thus, even if the Search Warrant did lack particularity, the good faith doctrine would preclude suppression of the seized evidence.

C. *Review and Retention of the Seized Material*

Mendlowitz further argues that the seized ESI was not properly reviewed to identify documents responsive to the Search Warrant and that the Government should return or destroy the non-responsive portions of the seized evidence. The Government maintains that its seizure and retention of the ESI complied with the Fourth Amendment and that, when asked by CPS, it returned portions of the seized materials.

1. Applicable Law

The Fourth Amendment’s “overarching purpose is to ensure that ‘those searches deemed necessary should be as limited as possible.’” *United States v. Cioffi*, 668 F. Supp. 2d 385, 390 (E.D.N.Y. 2009) (quoting *Coolidge*, 403 U.S. at 467). In addition to requiring particularity and

forbidding overbreadth, the manner in which the government executes a warrant must comport with the Fourth Amendment’s “reasonableness” standard. *United States v. Metter*, 860 F. Supp. 2d 205, 212 (E.D.N.Y. 2012).

Courts recognize that searches of electronic evidence often cannot be accomplished during an on-site search. Under Federal Rule of Criminal Procedure 41(e)(2)(B), a warrant may “authorize the seizure of electronic storage media or the seizure or copying of electronically stored information.” Fed. R. Crim. P. 41(e)(2)(B). The Rule provides that “[u]nless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant.” *Id.* Although “there is no established upper limit as to when the government must review seized electronic data to determine whether the evidence seized falls within the scope of a warrant,” courts have found that “the Fourth Amendment requires the government to complete its review . . . within a ‘reasonable’ period of time.” *Metter*, 860 F. Supp. 2d at 215; *see also United States v. Alston*, No. 15 Cr. 435 (CM), 2016 WL 2609521, at *3 (S.D.N.Y. Apr. 29, 2016) (“While Rule 41 prescribes no particular time period for data extraction in these circumstances, the time needed to complete off-site copying or review is subject to the rule of reasonableness.”). However, there is no “‘one size fits all’ time period.” *United States v. Ganias*, 755 F.3d 125, 136 (2d Cir. 2014) (“*Ganias I*”) (noting Rule 41 recognizes severable variables—e.g., storage capacity of media, difficulties created by encryption or electronic booby traps, and computer-lab workload—that may influence the duration of a forensic analysis), *rehearing en banc*, 824 F.3d 199 (2d Cir. 2016) (“*Ganias II*”).

2. Application

a. Review of Seized Material

I find that the seized ESI was reviewed off-site in compliance with the Fourth Amendment. Government agents properly and selectively executed the Warrant, reviewed the evidence over a reasonable period of time, and provided defense counsel with discovery indices and letters that ultimately separated 1,830 responsive documents from a larger universe of seized materials. With regard to the timing, I find that the Government exercised the appropriate diligence by beginning its review in approximately October 2015, two months after the execution of the Search Warrant and after the relevant portions of the hard drives had been copied onto text-searchable software platforms, and completing the review before the return of the Indictment in April 2017.

Nothing about the seizure of certain CPS servers and computers for later review was improper. Rule 41 provides that, absent any limitation in the warrant itself, the government may seize “electronic storage media or . . . electronically stored information” for “a later review of the media or information consistent with the warrant.” Fed. R. Crim. P. 41(e)(2)(B). Rule 41 also explicitly authorizes the government to retain a copy of electronic media seized pursuant to a warrant. *See* Fed. R. Crim. P. 41(f)(1)(B) (“The officer may retain a copy of the electronically stored information that was seized or copied.”); *see also Garias II*, 824 F.3d at 231–32. Consistent with Rule 41, the Search Warrant authorized law enforcement agents to seize computers and other electronic devices that might contain evidence falling in the categories enumerated in the Warrant. (*See* SW Attach. B.)

Moreover, the Government’s review process was appropriate and fully in keeping with the Search Warrant. First, the Warrant did not require any specific procedure for review of the

ESI, but expressly authorized “various techniques to locate information responsive to the warrant,” along with a list of examples of appropriate methods of review. (*Id.*) Second, the eighteen-month length of the review process was not incongruous with the need for thorough review of a universe of documents that Mendlowitz himself acknowledges was exceedingly large. “Numerous cases hold that a delay of several months or even years between the seizure of electronic evidence and the completion of the government’s review of it is reasonable.” *United States v. Jarman*, 847 F.3d 259, 267 (5th Cir. 2017) (upholding a twenty-three-month long review of electronic evidence) (internal quotation marks omitted). “[C]omputer searches are not, and cannot be subject to any rigid time limit because they may involve much more information than an ordinary document search, more preparation and a greater degree of care in their execution.” *United States v. Triumph Capital Grp.*, 211 F.R.D. 31, 66 (D. Conn. 2002); *see also United States v. Gorrell*, 360 F. Supp. 2d 48, 55 & n.5 (D.D.C. 2004) (upholding ten-month delay in analysis of computer hard drives by agency in a drug case where only five devices were recovered); *cf. Metter*, 860 F. Supp. 2d at 215 (finding a violation after fifteen months where the government had not even begun to conduct its review of the evidence and had “no plans whatsoever to begin review of that data”).¹³ I find that the extraction and review period is reasonable under the circumstances of this case.

b. Retention of Seized Material

The Government has also properly retained the electronic devices that remain in its possession. As a general matter, the government has an interest in preserving seized electronic devices for purposes of introducing data stored therein at trial. *See, e.g., Gacias II*, 824 F.3d at

¹³ Mendlowitz also argues that “an evidentiary hearing will assist in understanding whether the Government is still engaged in reviewing non-responsive evidence.” (Mendlowitz Mem. 22.) However, the Government has stated that it completed its review prior to obtaining the Indictment in April 2017. (See Smith Dec. Ex. 9.) An evidentiary hearing is not necessary.

215 (“Preservation of the original medium or a complete mirror may therefore be necessary in order to safeguard the integrity of evidence that has been lawfully obtained or to authenticate it at trial.”); *United States v. Carpenter*, No. 13-CR-226(RNC), 2015 WL 9461496, at *6–7 (D. Conn. Dec. 24, 2015) (remarking that the government had a “legitimate interest in retaining the documents for review and possible use as evidence at a trial”). The Government’s interest in maintaining custody of the devices, coupled with the fact that Mendlowitz has not demonstrated any need for their return, makes their continued retention reasonable in this instance. *See Carpenter*, 2015 WL 9461496, at *7 (finding retention reasonable in part because defendant had not “shown that he needs any of the documents in order to prepare his defense or for some other legitimate purpose”).

For similar reasons, I find that the Government is not required to divest itself of information contained on the devices. The Government has acknowledged that, following its review of the electronically stored information, it identified certain files responsive to the Warrant and certain folders containing irrelevant material, which it has segregated and has not continued to review. (Gov. Mem. 42.) Such efforts suffice for purposes of executing the Warrant, because complete digital segregation is often not reasonable or possible. *See, e.g.*, *Ganias II*, 824 F.3d at 213 (“[I]nterspersion of [electronically stored data on hardware] may affect the degree to which it is feasible, in a case involving search pursuant to a warrant, to fully extract and segregate responsive data from non-responsive data.”); *United States v. Lumiere*, No. 16 Cr. 483, 2016 WL 7188149, at *4 (S.D.N.Y. Nov. 29, 2016) (“*Ganias* acknowledges that meaningful digital segregation may well be impossible.”).

Mendlowitz’s reasoning in support of his argument that the retained material must be returned is unpersuasive. Mendlowitz fails to cite controlling precedent requiring the

Government to divest itself of non-responsive ESI from an electronic device prior to trial. Mendlowitz relies exclusively on the Second Circuit panel’s decision in *Ganias I*, which found that “the government’s retention of copies of Ganias’s personal computer records for two-and-a-half years deprived him of exclusive control over those files for an unreasonable amount of time.” 755 F.3d at 137. However, on rehearing en banc, the Second Circuit vacated the panel’s decision and, without reaching the question of whether the government violated the Fourth Amendment, found that executing agents relied on the warrant in good faith and suppression was therefore not warranted. *Ganias II*, 824 F.3d at 225–26. Mendlowitz also contends that the Government’s continued retention of ESI is unreasonable in light of the fact that defense counsel agreed to stipulate to the authenticity of the information. (Mendlowitz Reply 15.) This is equally unpersuasive, and Mendlowitz does not cite case law to the contrary. *See Ganias II*, 824 F.3d at 215 & n.33 (noting that “[e]ven after copying data from a computer or piece of storage media, digital investigators generally retain the original evidential item in a secure location for future reference” and that “[t]he weight of digital evidence admitted at trial . . . may be undermined by challenges to its integrity—challenges which proper preservation might have otherwise avoided”).

Finally, even if the Government’s retention of electronic media containing both responsive and non-responsive data was unreasonable, blanket suppression, as Mendlowitz advocates, would not be appropriate and is not supported by the law. “[W]hen items outside the scope of a valid warrant are seized, the normal remedy is suppression and return of those items, not invalidation of the entire search.” *United States v. Matias*, 836 F.2d 744, 747–48 (2d Cir. 1988). “[T]he drastic remedy of the suppression of *all* evidence seized is not justified unless those executing the warrant acted in flagrant disregard of the warrant’s terms.” *Id.* (internal

quotation marks omitted). “Government agents ‘flagrantly disregard’ the terms of a warrant so that wholesale suppression is required only when (1) they effect a widespread seizure of items that were not within the scope of the warrant, and (2) do not act in good faith.” *United States v. Shi Yan Liu*, 239 F.3d 138, 140 (2d Cir. 2000) (internal quotation marks omitted). Here, neither prong is applicable.

Far from flagrantly disregarding the Search Warrant, the Government instead abided by it. The Government plainly had authority to seize the devices at issue, and then, consistent with the terms of the Warrant, conduct an extraction and review from the devices to determine whether they contained responsive material. The Warrant did not, by its own terms, require the Government to use a particular protocol to search or segregate documents. It merely directed agents to review the seized devices for responsive evidence. (See SW Attach. B.) The Warrant authorized the Government to, among other things, “use various techniques to locate information responsive to the warrant, including . . . surveying various file ‘directories’ and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files) [and] performing key word searches through all electronic storage areas.” (*Id.*) That review process resulted in the identification of a modest collection of 1,830 responsive documents. As noted above, the Government retained the seized electronic evidence not to continue searching material deemed nonresponsive, but to accomplish certain investigative and litigation goals, including those discussed in *Ganias II*. Nor has the Government acted in bad faith. The Government imaged the devices, and reviewed their contents in a timely manner. Cf. *United States v. Debbi*, 244 F. Supp. 2d 235, 237–38 (S.D.N.Y. 2003) (finding lack of good faith where government overseized copious amounts of physical records, thereby depriving defendant of their use, and refused

multiple requests by the defendant and court to return items beyond the scope of the warrant), and subsequently returned various items to CPS.

For the foregoing reasons, I find that the Government has properly reviewed and retained the ESI at issue and, accordingly, Mendlowitz's motion seeking return of the seized material and/or suppression of that material is denied.

IV. Conclusion

For the foregoing reasons, and for the reasons stated on the record at the May 16, 2018 conference: (1) Defendants' motions for a bill of particulars and for identification of *Brady* material are denied; (2) Defendants' motions for the early production of lists of trial witnesses and trial exhibits is granted in part and denied in part; (3) Defendant Mendlowitz's motion for a list of co-conspirators is granted; and (4) Defendant Mendlowitz's motion to suppress evidence obtained pursuant to the Search Warrant is denied. Specifically, with regard to other requests made in Mendlowitz's motion: (1) the Government shall disclose Rule 404(b) evidence six weeks prior to jury selection and Mendlowitz shall provide his objections to the Government five weeks prior to jury selection; (2) motions in limine with regard to Rule 404(b) evidence and any other evidence shall be due four weeks prior to jury selection, with responses due three weeks prior to jury selection; (3) the Government shall begin production of material pursuant to *Giglio* and 18 U.S.C. § 3500 two weeks prior to jury selection and thereafter produce such material on a rolling basis so as to have completed production for all witnesses scheduled to testify in the first two weeks of trial by jury selection; (4) the Government shall provide a list of the witnesses it intends to call at trial at least two weeks prior to jury selection; (5) the Government shall begin production of its list of exhibits it intends to introduce as parts of its case in chief two weeks prior to jury selection and production shall be completed by jury selection, with the

understanding that circumstances my result in or require a certain number of exhibits being disclosed after jury selection; and (6) the Government shall produce a list of co-conspirators one week prior to jury selection.

The Clerk's Office is respectfully directed to close the open motions at Docket Entries 46 and 52.

SO ORDERED.

Dated: March 2, 2019
New York, New York


Vernon S. Broderick
Vernon S. Broderick
United States District Judge